Overview of E-Authentication

January 2006

E-Authentication: An Overview

- What is E-Authentication?
- Why is E-Authentication Important?
- What is a Credential?
- How Does E-Authentication Work? (User Perspective)
- How Does E-Authentication Work? (Technical Perspective)
- The Initial Program
- What's Next?
- Questions?

What Is E-Authentication?

E-Authentication is:

- An emerging, Government-wide, online identity validation service
- A service that will allow users to enter user IDs (identity credentials) from trusted providers to access Government and some private services online

Why Is E-Authentication Important?

- Improves access to FMCSA systems through the COMPASS program
  - E-Authentication will set the stage for simple sign-on in 2006
  - E-Authentication will be integrated into Agency systems from 2006
- Provides access to the E-Authentication Federation
  - Initial users will have access to sites being launched by members of the Federation, a collection of public and private organizations that will make their sites accessible to E-Authentication credential holders
  - FMCSA users with E-Auth credentials from other sources [e.g. Employee Express, Bank of America] will soon be able to use their credentials on FMCSA and other public and private Federation sites
- Satisfies the Office of Management and Budget's (OMB) Requirement
  - FMCSA has been designated as DOT's lead agency for meeting OMB's requirement for all Federal agencies to have one E-Authentication-enabled application
  - DOT has received a "Green" E-Government rating as a result of our success so far

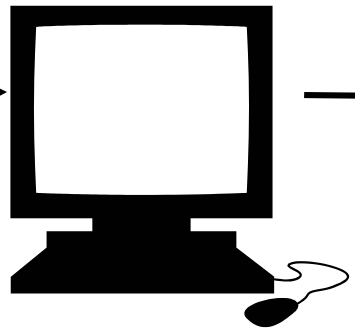
What is a Credential?

- A traditional credential (password/user ID) is replaced with one supplied by a "Credential Service Provider" (CSP)
  - ORC, Inc. has been chosen as the initial FMCSA CSP. ORC, Inc. will ensure that a user's identity has been verified (through the use of a social security number and a visual check by a Notary Public) before validating a special user ID/password combination
- CSP supplied credential would then be used on SAFER for the initial E-Authentication program
- Credential could then be used on other Government and private applications as they become available—provided that a user is authorized to use those applications.

How Does E-Authentication Work? (User Perspective)

Application User

Step 1



Access Point

Step 2

Credential Service Provider

Step 3

Agency Application

Step 1:

At access point (portal, agency Web site or credential service provider), user selects agency application and credential provider

Step 2:

- **User is redirected to selected credential service provider**
- **If user already possesses credential, user submits it for authentication**
- **If not, user acquires credential and then submits it for authentication**

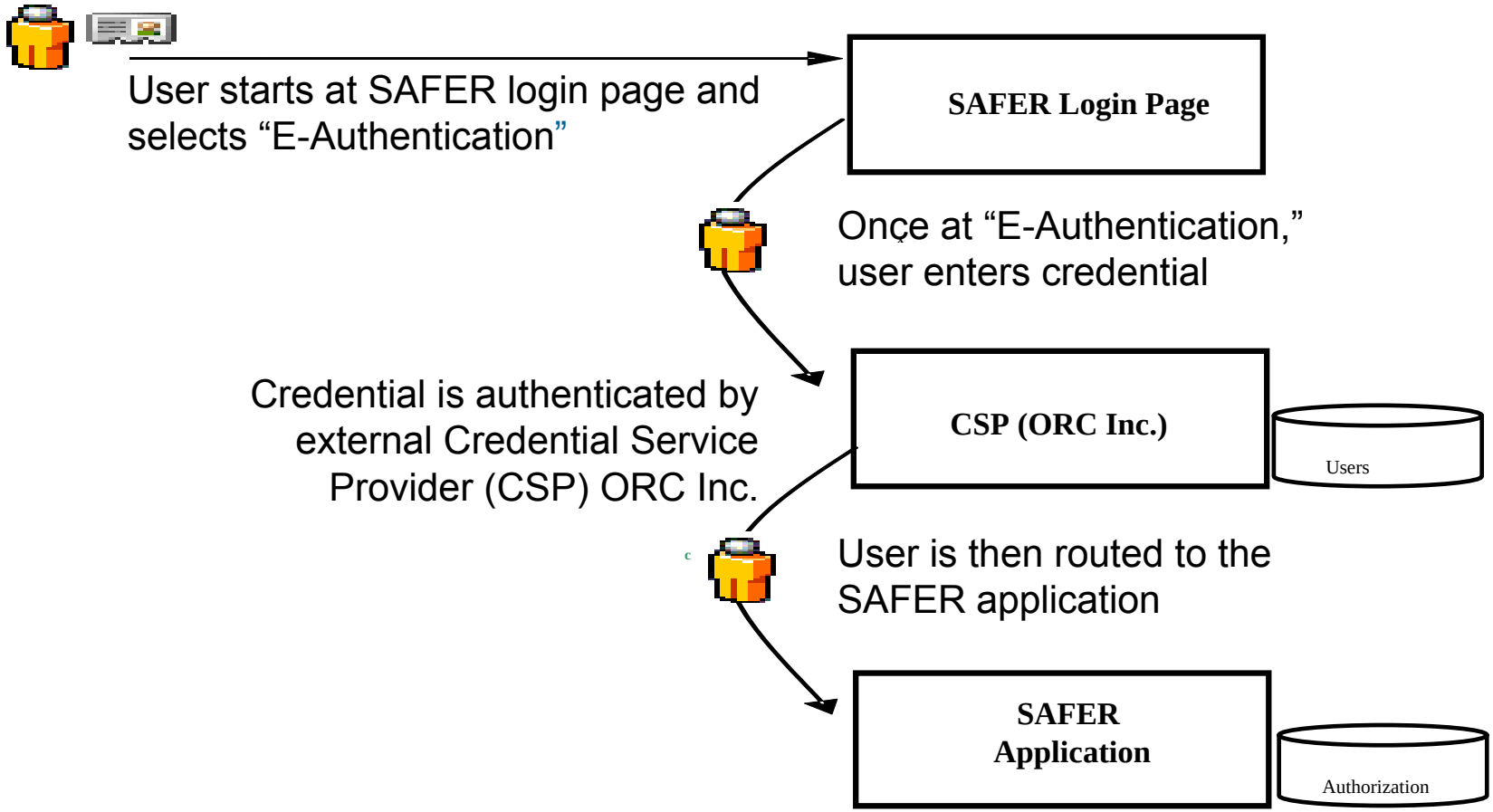
Step 3:

Credential service hands off authenticated user to the agency application selected at the access point

(Note: This is similar to the way we currently access Web sites)

How E-Authentication Works (Technical Perspective)

- FMCSA Initial E-Authentication Program will involve the SAFER system



The Initial Program

- Approximately 20 users
- Launch in December 2005
- Credentials issued by ORC, Inc. and used until agency-wide implementation of simple sign-on through the COMPASS program
- Users given access to Federation sites as they become available (though additional credentials may be required)

What's Next?

- E-Authentication becomes cornerstone of simple sign-on
- FMCSA secures Green status on E-Auth/E-Gov for DOT through 2006
- Federation begins to open new E-Authentication-enabled sites

Questions?

- For more information about E-Authentication, please e-mail: **Security@fmcsa.dot.gov**